INTERACTIVE **SOFTWARE**
**FEDERATION** OF EUROPE
*Representing the European video games industry*

# The Information Commissioner's Public Consultation on the Code for Age-Appropriate Design

## ISFE response

ISFE[1] represents the European video games industry. Our membership includes 16 major publishers of interactive software and trade associations in 18 countries throughout Europe which represent hundreds of game companies of all sizes. The video game industry is the fastest growing sector of the European content industry, with a revenue of €21 billion in 2018 and a growth rate of 15% in key European markets. Games are also a major driver of the European app economy: 75% of downloads on the Apple Store are games and 6000 apps are released daily on the Google Play Store. With a successful community of European and UK-based app developers and publishers affirming their strong position worldwide, mobile gaming is expected to represent 44% of industry growth in 2019[2].

ISFE welcomes the opportunity to provide feedback on the Draft ICO Code for Age-Appropriate Design ("ICO Code"). Due to the very short consultation period of only six weeks, ISFE is unable to properly assess the full impact of all aspects of the proposed requirements on our sector, nor does the time allow to consider the potential interplay between the draft ICO Code , the outcome of the consultation on the Online Harms White Paper and other government initiatives related to consumer protection. This is a complex and important area of policy which merits time and care. ISFE therefore calls for a continued dialogue with the ICO that will allow us to gather evidence for an in-depth analysis of each of the proposed standards and to consider all consequences on our sector, including unintentional ones.

### The Best Interest of the Child is the Video Game Industry's Primary Consideration

We strongly support the ICO Code's overall objective to ensure fair processing of children's data in compliance with the basic principles of the General Data Protection Regulation (GDPR). In particular, we are committed to the GDPR's principle approach that children need particular protection when their personal data are collected and processed because they may be less aware of the risks, consequences and safeguards concerned.

The video game industry is aware of the risks related to children in digital environments and understands the importance of establishing practical measure and safeguards. Our sector has undertaken a number of initiatives, which are summarised below, that go beyond mere compliance with the law and set self-regulatory standards to protect children's privacy, create a safer off- and online environment and promote involvement of parents and carers. These standards demonstrate our commitment to respect the rights of the child and those of the parents. They also demonstrate how we always put the best interest of the child as a primary

[1] See www.isfe.eu
[2] https://www.isfe.eu/data-key-facts/

consideration when products and services are being developed as was envisaged by Article 3 of the United Nations Convention on the Rights of the Child.

**Self-Regulatory Standards and Responsible Practices**

In 2003, the video game industry established the PEGI system which operates through a set of scientifically backed ethical standards in the form of a Code of Conduct[3]. The PEGI system is part of the industry's commitment to protect minors and behave responsibly where children are concerned. Each publisher that joins PEGI has to sign a Code of Conduct committing him to provide parents with objective, intelligible and reliable information regarding the suitability of a game's content. By signing the Code of Conduct, the publisher also undertakes to maintain a responsible advertising policy, provide opportunities for consumer redress, maintain community standards and adhere to stringent standards for a safe online gaming environment. These include the need to maintain an effective and coherent privacy policy which must encompass the responsible collection, distribution, correction, and security of the personal details of users who must be given the opportunity to comment on any perceived misuse of their personal details and therefore be fully advised as to ways, for example, of avoiding unsolicited or unwanted e-mail contact[4].

The PEGI system is recognised and implemented in English law. It is also recognised by the European Commission and considered as a model of European harmonisation in the field of minor protection and consumer transparency. It is overseen by a number of independent bodies such as the PEGI Council with officially designated representatives of the European Member States and Institutions, the PEGI Experts Group is comprised of specialists and academics in the fields of media, child psychology, classification & technology, and the PEGI Complaints Board and Enforcement Committee composed of independent experts. The content ratings themselves are given by two designated independent games rating authorities, the UK Video Standards Council (VSC) and the Netherlands Institute for Classification of Audiovisual Media (NICAM), who review and monitor all declarations by PEGI signatories.

In 2013, the industry established IARC, The International Age Rating Coalition, which comprises rating boards from Europe, North America, Brazil and Australia who have joined forces to provide a solution for the globalised market of apps collectively representing regions serving approximately 1.5 billion people. IARC has now been adopted by Google Play Store, Microsoft Windows Store, Nintendo® eShop and the Sony PlayStation® Store and informs the consumer about certain types of functionality in an app, such as in-app purchases, location data sharing, unrestricted internet access and the ability of users to interact.

The PEGI classifications are supported by sophisticated and robust parental control tools on a variety of devices and software applications that not only allow parents to control access to video game content based on 'their child's age and maturity but also allow them to manage and control how their children access the internet, share their data and interact with others online. Parents can set up accounts for their children providing them with a significant degree of control over their children's online activities, including managing with who and how the child

[3] https://pegi.info/pegi-code-of-conduct
[4] Article 9.4 of the PEGI Code

communicates and whether user-generated content can be shared. The parental control tools provided by one ISFE member have even been officially recognised under the German youth protection regime – it is thus the first youth protection programme for proprietary platforms that has received this level of recognition in Germany, which has been considered a milestone for technical youth protection by the Commission for the Protection of Minors in the Media[5].

Even before the GDPR had entered into force, the industry adopted Privacy by Design as a key design principle when new products and systems are being developed. Game play data, for instance, is usually collected and stored in a way that does not allow companies to identify the player directly by applying technical and organisational measures to prevent easy linking between the game play dataset and the players' account information. Our companies have also since long endorsed the use of pseudonymised data as a valid way to protect identity of underaged users.

We feel encouraged by the 16 standards of age-appropriate design that have been proposed in the draft ICO Code as they effectively recognize the work we have been doing so far. However, we are equally concerned that some aspects of the detailed guidance on what these standards mean and how they can be implemented in practice may go beyond the overall objective of ensuring fair processing in compliance with the GDPR. Some guidelines may even have a contrary effect on the protection of children's privacy or are based on misconceptions about how data is processed in our sector. Our concerns relate in particular to following standards in the ICO Code: age-appropriate application, detrimental use of data, nudge techniques, default settings, geolocation, profiling and parental controls.

**The Scope of Age-Appropriate Design**

The draft ICO Code allows for no proportionality with regard to the intended audience of a service, the type of content or service, the likely share of the audience that is children, or the size of the business that is delivering the service. It requires companies to consider the age range of children likely to access the service and apply the standards in the ICO Code to all users, unless robust age-verification mechanisms can distinguish children from adults. The ICO Code however does not explain how the age range of children that are "*likely to access*" a service should be established. It does not clearly define this concept, nor does it propose a methodology to establish with a sufficient level of certainty the probability that a certain age range of children is accessing a service.

ISFE is concerned that the lack of a clear methodology in this respect would create uncertainty for video game publishers about the level of protection that they need to apply on their services. Age classification cannot be of any help in this respect. While video games are consumed by a wide variety of consumers of all ages age classifications only provide for a minimum age for which the content of a given product is considered suitable and not for information on whether the game can be played by this particular age group, nor whether this group is "likely" to access the game. A chess game, for instance, will always be classified as suitable for all ages, although very young children will find it too difficult to play.

[5] https://www.kjm-online.de/service/pressemitteilungen/meldung/news/meilenstein-im-technischen-jugendmedienschutz/

Annex A of the ICO Code provides for a guide of age ranges and development stages that is supposed to help assess what is broadly appropriate for children of that age and what might be expected at each stage of development. The proposed guide would however only be of limited benefit to companies and introduce further uncertainty as intellectual capacities, skills and behaviours can vary considerably between different children, with cultural and social differences playing also a part in child development. Furtheremore, this will be an increased burden on businesses to build such provisions into current services, where considerabe development time would be required to design and implement changes required by the ICO Code.

Adding to this confusion is that the draft ICO Code requires companies to consider that all users under 18 are children while the provisions of the CAP Code and relevant guidance clearly define children as under 16 and only apply to marketing communications "addressed to, targeted directly at or featuring children", a higher standard than the ICO Code. Furthermore, the Data Protection Act from which this Code derives specifies the age at which consent for data processing can be given as 13. Many organisations (particularly larger ones) that provide global online services from the UK, would have to apply the ICO Code to children accessing services from outside the UK, even where those laws/regulators (including European laws/regulators) may not impose the same requirements.

Any online service with any underaged users will effectively face the choice of applying the ICO Code for all users (including adult ones) by default, building separate child-appropriate and adult versions of the service, or excluding children from their services altogether. While the second option would confuse consumers, the latter will be the most economically viable option for services with a predominantly but not exclusively adult audience. In the app market, for instance, developers can rely on their platform partners' age gates, and typically do not have any robust systems designed to separate the players by age. For such developers, the choice between a significant investment in changing their services for a very small share of the audience or blocking those audience members altogether will be easily made. Uncertainty about how to apply the draft ICO Code will push also services with a more mixed audience to such a solution, effectively making the majority of online services unavailable to under-18s.

Recommendation: clarify the definition of "likely to appeal to children", and the age of application of the code, to allow services to take a proportionate, risk-based approach to its implementation by focusing their efforts where children are most likely to be found online.

It is also unclear which age-verification mechanisms can be applied to distinguish children from adults. The draft ICO Code clearly states that "asking users to self-declare their age or age range does not in itself amount to a robust age-verification mechanism under this code" and that companies must be "able to demonstrate that children cannot easily circumvent the age checks". It does however not indicate which mechanisms would be sufficiently robust and in compliance with data protection law to satisfy ICO standards. It merely recommends companies to consider using "a trusted third-party service" without providing any concrete examples. It is questionable whether such services would be able to operate legally in the UK. They would have to collect the date of birth and contact information for the child including potentially also a copy of the ID card or passport of the child and of the parent, in case parental consent is required.

Consequently, the amount of personal data that is processed about the child, and potentially also the risk to the security of the processed data would be increased which may contradict GDPR requirements on data minimisation. It is also unclear what appropriate documents would suffice for age verification in a global context.

The draft ICO Code correctly identifies that "age-verification tools are still a developing area" and promises that "the Commissioner will support work to establish clear industry standards and certification schemes". However, as long as there is not a single system that offers sufficient assurance to be applied as a one size fits all solution on a national basis the requirements in the ICO Code cannot be implemented. In addition, the videogames industry is essentially an international business so that solutions that may work only in individual countries do not seem feasible.

Recommendation: provide clear and concrete examples of mechanisms that can be considered appropriate methods for verifying the age of children and provide at the same time the necessary flexibility and cost effectiveness.

**Detrimental Use of Data**

ISFE agrees with the ICO position that personal data of children should not be used in ways that that are detrimental to children's physical or mental health and wellbeing. The ICO goes further by stating that even in the absence of conclusive evidence a pre-cautionary approach should be taken to the processing of children's personal data in ways that have been formally identified as requiring further research or evidence to establish whether or not they are detrimental to the health and wellbeing of children.

In this context, the ICO refers to so-called "strategies used to extend user engagement", or "sticky features" that appear to include "mechanisms such as reward loops, continuous scrolling, notifications and auto-play features which encourage users to continue playing a game, watching video content or otherwise staying online". The ICO then bases itself on the UK Chief Medical Officers' Commentary on Screen-Based Activities on Children and Young People which identifies a need for further research and recommends that technology companies "recognise a precautionary approach in developing structures and remove addictive capabilities" to advise that companies "should "not use children's personal data to support these types of mechanisms and strategies".

ISFE would like to point out that these mechanisms have been characterised broadly but have not been properly defined. ISFE would like to receive further clarification on how they function and how they make use of children's personal data in order to assess whether they would be applicable to the video game sector at all. The UK Chief Medical Officers' Commentary on Screen-Based Activities on Children and Young People has clearly stated that there is no clear evidence of a causal relationship between screen-based activities and mental health problems and made its recommendation as part of a *potential* area of inclusion in a *voluntary* code of conduct[6]. In this context, it is worth noting that the video games industry has already included such a

[6] UK Chief Medical Officers' Commentary on Screen-Based Activities on Children and Young People see points 3.4 and 6.4.4

requirement in the PEGI Code of Conduct whereby signatories must advise users of online game play environments to take regular breaks[7]. In addition, the aforementioned parental control systems available for free on a variety of devices, including platforms operated by ISFE members, often contain features that allow parents to limit their child's daily play time and to define a "bedtime" after which the child cannot play anymore. More appropriate measures would therefore be to provide further education on the detrimental use of data to parents/legal guardians, who are more likely to ensure their children take the required breaks and regulate screen-based activities.

Recommendation: provide further detail on what "strategies used to extend user engagement" may look like in different contexts, alongside clear evidence demonstrating the harm caused to children and the justification for regulation of data processing related to such strategies.

**Nudge Techniques**

The ICO Code refers to these mechanisms again in the context of its chapter on so-called "nudge techniques". Nudge techniques are defined as design features which lead or encourage users to follow the designer's preferred paths in the user's decision making. The ICO recommends that these should not be used to encourage children to provide unnecessary personal data, turn off privacy protections, or extend use. It explains that "reward loops or similar techniques seek to exploit human susceptibility to reward, or anticipatory and pleasure-seeking behaviours in order to keep children engaged in the service to facilitate and maximise collection of personal data."

The ICO seems to imply that online services only seek to encourage users to stay actively engaged with a service to maximise the amount of personal data that can be collected. This is not the case for the video games industry. Rewarding users for progressing within a game is part of the industry's DNA and a basic condition to ensure that the gaming experience remains competitive and enjoyable. The data generated by the players' activity is most commonly only collected and analysed to identify software errors and make adjustments to improve the player experience. It is deliberately processed in a way that does not allow to identify the user and it would therefore fall outside the scope of the applicable legal framework of the ICO Code.

Recommendation: clarify that restriction of 'nudge techniques' under this Code only applies to the collection of personal data and/or privacy concerns, and not to the design of services to make them engaging for users.

**Default Settings**

The GDPR requires that companies by default should not collect any more personal data than needed for each processing purpose or make users' personal data visible to indefinite numbers of other users[8]. This has led the ICO to conclude that "any optional, more intrusive, uses of personal data, including any uses designed to personalise the service have to be individually selected and activated by the child". It is important to point out in this context that personalisation of a service does not necessarily need to be based on data that allows to identify

[7] Article 9.6 of the PEGI Code of Conduct
[8] Article 25.2 GDPR

the user. Video game companies often apply technical and organizational measures to prevent linking of the gameplay data with identifiable information. Such anonymised or pseudonymised datasets are much safer to handle but still allow to personalise the user experience. We would ask the ICO to recognise these techniques in the ICO Code.

ISFE however would like to caution that the GDPR's privacy by default requirement does not mean that parental controls must be switched on by default. Our sector generally encourages parents to accompany their children when experiencing videogames and supports the use of active choice. This means that we believe that it is more effective to ask parents to make a series of choices as to the level of parental control and filtering on a device, making them mentally engage with what is appropriate for their family, than to simply have all such controls switched on automatically when they first use the device. An active choice policy strengthens the child-parent interaction and enables the parents to best protect and educate their child.

**Geolocation**

The ICO extends its recommendation on applying by default the highest privacy settings also to geolocation data. It says that geolocation options should be switched off "unless one can demonstrate a compelling reason for geolocation, taking account of the best interests of the child." ISFE wants to point out that geolocation is often used as a security measure such as to combat fraudulent online activities. It is an important tool for ensuring that an online service is safe and secure which is why some services may activate it by default. This should be counter-balanced against the potential of misuse of such data or the perceived loss of privacy. In addition, it is sometimes also used to understand the interaction of visitors with products and services at live events, such as conferences and exhibitions.

**Profiling**

ISFE cannot support the ICO's recommendation that companies should not use profiling on children by default. It is our understanding of Article 22 and Recitals 38 and 71 of the GDPR that this type of automated processing on children is not prohibited as long as it does not produce legal or similarly significant effects on the child and protection measures for children are in place. Profiling might, for instance, help improve the game experience by fixing areas of a game that prove problematic to progression or remember content that was recently played.

We strongly agree with the ICO that appropriate measures need to be in place to protect the child from any harmful effects (and in particular inappropriate content) when profiling is used. In this context we would like to reiterate that the video game sector has deployed an array of tools to protect children from unsuitable content. The PEGI Code of Conduct signatories must ensure that community standards are implemented to ensure the protection of minors from unsuitable content and behaviour associated with these online environments. This includes requiring appropriate reporting mechanisms to be in place to allow players to notify such content or conduct and that offensive, racist, degrading, corrupting, threatening or obscene content is always taken down, including in chatrooms.

**Parental Control Tools**

The ICO requires that a child should receive age appropriate information, including by audio and video, about privacy policies and the functioning of parental controls and that an obvious sign should be displayed when its online activity or location is being monitored. Our sector has a track record of communicating to parents, guardians and players to promote the use of parental controls whereby we take great care to emphasize that these tools are best utilised by parents and children working together to understand games and game play, rules and boundaries. We have also conducted several public awareness campaigns to inform parents about on how to set fair rules, and how to start a dialogue and take an interest in their children's online activities.

A survey conducted in April 2018, commissioned by ISFE from Ipsos Mori, shows that parents are indeed in dialogue with their children as regards in-game spending, with only 2% of parents not monitoring the spending of their children within a game[9]. ISFE believes that informing children about online tracking tools should be best done in a direct child-parents interaction. While audio-visual features would be unworkable for apps, an online sign or icon as proposed in the draft ICO Code has the potential to confuse. They should not substitute a face to face conversation. It is much more effective to engage with children and explain what is appropriate.

Furthermore, icons or online signs showing children some parental controls are on may have unforeseen impacts for example, if children know that their online activity is being monitored or controlled, then they may try and circumvent such measures and put them at extra risk online, which defeats the purpose of what the ICO Code is trying to achieve.

**Conclusion**

ISFE supports the ICO Code's principal approach of always putting the best interests of the child as prime consideration. While our sector has already been implementing large parts of the guidance through its self-regulatory standards and responsible practices, we are concerned that the ICO Code's broad scope and vague definitions and guidance can cause confusion and legal uncertainty which may lead to the exclusion of underaged users by many online services, even if they do not have a predominantly adult audience.

We are also concerned about the wider economic impact of this broad scope on the digital economy as cost of implementation can be severe. The ICO Code requires significant resources, especially in regard to age verification, which may place more pressure on smaller businesses and start-ups as well as larger businesses in terms of implementing such designs into current well-established services, creating further barriers to growth and thus stifle innovation. It may also have a negative effect on consumer choice, as older content and platforms may be removed from the UK market if the cost of compliance outweighs any benefit of keeping it available. ISFE therefore calls for a continued dialogue with the ICO that will allow us to gather evidence for an in-depth analysis of each of the proposed standards and to consider all consequences on our sector, including unintentional ones.

[9] https://www.isfe.eu/news/research-majority-of-parents-control-childs-in-game-spending